ANNALES

DE

L'INSTITUT FOURIER

Yuri BILU, Pierre PARENT & Marusia REBOLLEDO

**Rational points on $X_0^+(p^r)$**

Tome 63, n° 3 (2013), p. 957-984.

<http://aif.cedram.org/item?id=AIF_2013__63_3_957_0>

Ann. Inst. Fourier, Grenoble
**63**, 3 (2013) 957-984

# RATIONAL POINTS ON $X_0^+(p^r)$

**by Yuri BILU, Pierre PARENT & Marusia REBOLLEDO (*)**

*To the memory of Fumiyuki Momose*

Abstract. — Using the recent isogeny bounds due to Gaudron and Rémond we obtain the triviality of $X_0^+(p^r)(\mathbb{Q})$, for $r > 1$ and $p$ a prime number exceeding $2 \cdot 10^{11}$. This includes the case of the curves $X_{\mathrm{split}}(p)$. We then prove, with the help of computer calculations, that the same holds true for $p$ in the range $11 \leqslant p \leqslant 10^{14}$, $p \neq 13$. The combination of those results completes the qualitative study of rational points on $X_0^+(p^r)$ undertook in our previous work, with the only exception of $p^r = 13^2$.

Résumé. — En utilisant les récentes bornes d'isogénies obtenues par Gaudron et Rémond, nous prouvons la trivialité de $X_0^+(p^r)(\mathbb{Q})$, pour $r > 1$ et $p$ un nombre premier supérieur à $2 \cdot 10^{11}$, ce qui inclut le cas des courbes $X_{\mathrm{split}}(p)$. Nous montrons ensuite, avec l'aide de calculs sur machine, la même propriété pour $p$ dans l'intervalle $11 \leqslant p \leqslant 10^{14}$, $p \neq 13$. La combinaison de ces résultats complète l'étude qualitative des points de $X_0^+(p^r)$ entreprise dans nos travaux précédents, à la seule exception du cas $p^r = 13^2$.

## 1. Introduction

For a prime number $p$ and an integer $r > 1$, let $X_0(p^r)$ be the usual modular curve parameterizing geometric isomorphism classes of generalized elliptic curves endowed with a cyclic isogeny of degree $p^r$, and let $X_0^+(p^r) := X_0(p^r)/w_{p^r}$ be its quotient by the Atkin-Lehner involution. When $r = 2s$ is even, $X_0^+(p^{2s})$ is $\mathbb{Q}$-isomorphic to the modular curve known as $X_{\mathrm{split}}(p^s)$ (see (2.3), Section 2 of the present article). The curves $X_0^+(p^r)$

*Keywords:* Elliptic curves, modular curves, rational points, Runge's method, isogeny bounds, Gross-Heegner points.
*Math. classification:* 11G18, 11G05, 11G16.
(*) Yuri Bilu was supported by the ANR grant HAMOT, the Erasmus Mundus ECW grant, and the Erasmus Mundus ALGANT program. Pierre Parent was supported by the ANR grant ARIVAF. Marusia Rebolledo was supported by the ANR grant Modunombres.

have motivated a number of works, dating back at least to Mazur's foundational paper [22], where the case of $X_{\mathrm{split}}(p)$ was tackled. Momose then obtained significant results in [26] and [27].

In [6, 5] we proved that for some absolute constant $p_0$, the only rational points of $X_0^+(p^r)$ with $p > p_0$ and $r > 1$ are trivial, that is, the unavoidable cusps and CM points. One easily checks the existence of degeneracy morphisms $X_0^+(p^{r+2}) \to X_0^+(p^r)$ which show that it is sufficient to settle the cases $r = 2$ and 3 (see (2.1), Section 2). Our method uses three main ingredients: an integrality statement for non-cuspidal rational points (Mazur's method), an upper bound for the height of integral points (Runge's method), and a lower bound for the height of rational points (isogeny bounds, obtained by the transcendence methods). The combination of those yields inequalities of the following shape for the height of a (non-cuspidal and non-CM) rational point $P$:

$$c\,p < \mathrm{h}(P) < 2\pi\sqrt{p} + O(\log p) \qquad (r = 2), \tag{1.1}$$

$$c'p^{3/2} < \mathrm{h}(P) < 24p\log p + O(p) \qquad (r = 3), \tag{1.2}$$

where $c$ and $c'$ are positive constants. This of course yields a contradiction when $p$ exceeds certain $p_0$, but the (implicit) value for $p_0$ in [6, 5] was extremely large, due to the huge size of the constants $1/c$ and $1/c'$ furnished by the transcendence theory.

In previous works [29, 31] we had developed very different methods leading to the same triviality results for primes in certain congruence classes. We were not able to make those earlier techniques prove triviality of integral points for almost all primes; on the other hand, they are very well fit for dealing with small primes $p$.

The aim of the present paper is therefore twofold. First we make the above inequalities (1.1) and (1.2) completely explicit. We did not try to obtain the numerical value of $p_0$ in [6, 5], but a calculation shows that in both cases triviality of $X_0^+(p^r)(\mathbb{Q})$ was established for $p$ exceeding $10^{80}$ (which is supposed to be approximately the number of atoms in the visible universe). Now, thanks to the work of Gaudron and Rémond [15], who obtained drastic numerical improvements of classical isogeny bounds, we can size this down to the much more manageable $p \geqslant 1.4 \cdot 10^7$ for $r = 2$ and $p > 1.7 \cdot 10^{11}$ for $r = 3$.

The second aim of this article is then to develop an algorithm based on the Gross vectors method [29, 31] and to explain how to use it on a computer to rule out primes in the range $11 \leqslant p \leqslant 10^{14}$, $p \neq 13$. This results in the following

THEOREM 1.1. — *The points of $X_0^+(p^r)(\mathbb{Q})$ are trivial for all prime numbers $p \geqslant 11$, $p \neq 13$, and all integers $r > 1$.*

It is perhaps worth stressing here that, even if the use of a computer was forced by the important range of primes we had to consider, the computations themselves are very elementary, so that it takes only a few minutes to rule out a given prime by hand - even much beyond our bound $10^{14}$. We refer the skeptical reader to Section 5.

For the remaining very small primes our methods break down, but ad hoc studies almost completely cleaned the situation up, see [27, Theorem 3.6], [28, Theorems 0.1 and 3.14], and [14, Section 10]. Precisely:

- for $p = 2$ we have $X_0^+(2^r) \simeq \mathbb{P}^1$ for $2 \leqslant r \leqslant 5$ (the corresponding curves having thereby infinitely many $\mathbb{Q}$-points) and $X_0^+(2^r)(\mathbb{Q})$ is trivial for $r \geqslant 6$;
- for $p = 3$ we have $X_0^+(3^r) \simeq \mathbb{P}^1$ for $2 \leqslant r \leqslant 3$ and $X_0^+(3^r)(\mathbb{Q})$ is trivial for $r \geqslant 4$;
- for $p = 5$ we have $X_0^+(5^2) \simeq \mathbb{P}^1$, the curve $X_0^+(5^3)$ has one well-described non-trivial $\mathbb{Q}$-point [14, Section 10] and $X_0^+(5^r)(\mathbb{Q})$ is trivial for $r \geqslant 4$;
- for $p = 7$ we have $X_0^+(7^2) \simeq \mathbb{P}^1$ and $X_0^+(7^r)(\mathbb{Q})$ is trivial for $r \geqslant 3$;
- for $p = 13$ the set $X_0^+(13^r)(\mathbb{Q})$ is trivial for $r \geqslant 3$.

The only remaining question mark therefore concerns the curve $X_0^+(13^2) \simeq X_{\mathrm{split}}(13)$. It has genus 3 (so only finitely many rational points). Galbraith [13] and Baran [3] spotted seven (trivial) points, which, as they conjecture, exhaust $X_0^+(13^2)(\mathbb{Q})$, but this still has to be checked. We continue that discussion of the level $13^2$ case in Remark 5.11.

On the other hand, the question for the curves $X_0^+(p)$ remains, as far as we know, essentially open, apart from some partial or experimental results (see, for instance, [13, 16]). For prime level our methods indeed fail for deep reasons akin to the ones that make the case of $X_{\mathrm{nonsplit}}(p)$ so difficult (see, for instance, the introduction to [6]).

The problem of describing points over higher number fields is also extremely open (as it is a fortiori the case for the curves $X_0(N)$). As explained in [7, 4] one can explicitly bound integral and even $S$-integral points over arbitrary number field using Baker's method, but these bounds are quite huge and not very useful because of lack of integrality results.

Finally, our techniques should at least partially extend to curves $X_0^+(N)$ where $N$ has several prime factors (or even curves $X_0(N)/W$, where $W$ is the full group generated by the Atkin-Lehner involutions, at least in the

easier case where $N$ is not square-free). We plan to pursue this study in forthcoming works.

Let us recall two immediate consequences of Theorem 1.1 for the arithmetic of elliptic curves. The first concerns Serre's uniformity problem over $\mathbb{Q}$ [32, 6]. Recall that to an elliptic curve over a field $K$ and a prime number $p$ (distinct from the characteristic of $K$) one associates the Galois representation $\rho_{E,p}\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Serre [32] proved that, given a non-CM elliptic curve $E$ defined over a number field $K$, there exists $p_0 = p_0(E, K)$ such that for $p > p_0$ the representation $\rho_{E,p}$ is surjective. He asked if $p_0$ can be made independent of $E$. In particular, in the case $K = \mathbb{Q}$ (which will be assumed in the sequel) it is widely believed that $p_0 = 37$ would do:

> *Let $E$ be a non-CM elliptic curve over $\mathbb{Q}$, and $p > 37$ a prime number; is it true that the associated Galois representation is surjective?*

As explained in the introduction to [6], to answer this question affirmatively it suffices to show that the image of the Galois representation is not contained in the normalizer of a (split or non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Since elliptic curves over $\mathbb{Q}$ for which the image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup are parameterized by the $\mathbb{Q}$-points on the curve $X_{\mathrm{split}}(p) \simeq X_0^+(p^2)$, an immediate consequence of Theorem 1.1 is the following improvement of the main result of [6].

Corollary 1.2. — *Let $E$ be an elliptic curve over $\mathbb{Q}$ without complex multiplication and $p$ a prime number, $p \geqslant 11$, $p \neq 13$. Then the image of the Galois representation $\rho_{E,p}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is not contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

Another application of Theorem 1.1 concerns elliptic $\mathbb{Q}$-curves. Recall that an elliptic curve *with* complex multiplication, defined over $\bar{\mathbb{Q}}$, is isogenous to any of its conjugates (over $\mathbb{Q}$). A $\mathbb{Q}$-*curve* is an elliptic curve *without* complex multiplication over $\bar{\mathbb{Q}}$ with the same property, that is, isogenous to each of its conjugates over $\mathbb{Q}$. This notion was first introduced by Gross (in the setting of CM curves) in [17]; for more about this concept we refer in particular to the work of Elkies [11]. When a $\mathbb{Q}$-curve is *quadratic* (that is, defined over a quadratic field), we say that it *has degree $N$* if there is a cyclic $N$-isogeny from the curve to its only non-trivial conjugate. For concrete examples of quadratic $\mathbb{Q}$-curves see, for instance, [14] and the

references therein. It is known that quadratic $\mathbb{Q}$-curves of degree $N$ are parameterized by the non-CM rational points of the curve $X_0^+(N)$, see [5, beginning of Section 7]. Hence Theorem 1.1 has the following consequence, improving on the main result of [5].

COROLLARY 1.3. — *Let $p$ be a prime number, $p \geqslant 11$ and $p \neq 13$. Then for $r > 1$ there does not exist quadratic $\mathbb{Q}$-curves of degree $p^r$.*

**Plan of the article.** The material is organized as follows. Section 2 is devoted to recalling general facts on modular curves. In Section 3 we make the upper bounds in (1.1) and (1.2) explicit. In Section 4 we deduce the explicit lower bounds in (1.1) and (1.2) from the Gaudron-Rémond version of the isogeny theorem. The method and computations for small primes are explained in Sections 5 and 6. Let us finally note that, due to the nature of our proofs, the cases $r = 2$ and $r = 3$ are not completely similar, so we often prefer deal with each case separately, at the expense of some repetitions.

**Acknowledgments.** It is a pleasure to thank Éric Gaudron and Gaël Rémond for their efficiency in proving isogeny bounds which were even better than what they had promised, and for sharing their results with us. We are also grateful to B. Allombert, K. Belabas, A. Enge and C. Wuthrich for useful discussions. The PlaFRIM computational center in Bordeaux allowed us to make extensive computations, although what we eventually needed was less than we first feared. We thank the referee for his thorough reading and precise remarks, which helped us improving the presentation of this paper.

While working on this article we learned that Fumiyuki Momose had passed away, in April of 2010. His work has been a great source of inspiration for us, and we would like to dedicate this article to his memory.

**Convention.** In this article we use the $O_1(\cdot)$-notation, which is a "quantitative version" of the familiar $O(\cdot)$-notation: $A = O_1(B)$ means $|A| \leqslant B$.

## 2. Modular curves

We here briefly recall a few general and particular facts about modular curves, referring the reader to classical texts (for instance [33], [20] or [10]) for more details.

Throughout this article we denote by $\mathcal{H}$ the Poincaré upper half-plane and put $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Let $N$ be a positive integer. To any subgroup $G$ of

$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ one associates a modular curve, denoted by $X_G$, in the following way. Let $\widetilde{G}$ be the inverse image in $\mathrm{SL}_2(\mathbb{Z})$ of $G$ via mod $N$ reduction. Making $\widetilde{G}$ act on $\bar{\mathcal{H}}$ via homography we define the compact Riemann surface $X_G(\mathbb{C})$ as the quotient $\widetilde{G}\backslash\bar{\mathcal{H}}$. This complex algebraic curve admits a model, still denoted $X_G$, over $\mathbb{Q}(\zeta_N)$ (the number field generated by the $N^{\text{th}}$ roots of unity) and even over $K_G := \mathbb{Q}(\zeta_N)^{\det G}$ (identifying $(\mathbb{Z}/N\mathbb{Z})^\times$ with $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$). Deligne and Rapoport [10] have then built models for $X_G$ over the ring of integers $\mathcal{O}_{K_G}$ of $K_G$. When speaking of integral models for modular curves, we systematically refer to those.

The $j$-invariant defines a (nonconstant) map over $K_G$ (or $\mathcal{O}_{K_G}$) from $X_G$ to $X(1)$, the modular curve associated with the trivial group. The latter is known to have genus 0, and $j$ is one of its parameters. The images of elements of $\mathbb{P}^1(\mathbb{Q})$ in $\widetilde{G}\backslash\bar{\mathcal{H}}$ are called the *cusps* of $X_G$. They are the inverse image by the function $j$ of the point $i\infty$ in $X(1)$, and they can be shown to actually belong to $X_G(\mathbb{Q}(\zeta_N))$. We denote by $Y_G$ the scheme $X_G$ deprived of the cusps (either as a curve, over $K_G$, or as an arithmetic surface, over $\mathcal{O}_{K_G}$, depending on the context). One knows that $Y_G$ (respectively, $X_G$) is a (coarse) moduli scheme parametrizing isomorphism classes of elliptic curves (respectively, generalized elliptic curves) endowed with a basis of the $N$-torsion points such that the image in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ defined by Galois action is contained in $G$.

The most familiar instances of such curves are those associated with the Borel group mod $N$, that is the group of upper triangular matrices. They are usually denoted by $X_0(N)$ and it follows from the above that they admit a model over $\mathbb{Z}$. They parameterize geometric isomorphism classes $(E, C_N)$ of elliptic curves $E$ endowed with a cyclic isogeny $C_N$ of degree $N$. For each prime $p$ dividing $N$, write $p^r$ for the maximal power of $p$ dividing $N$. One can define a so-called Fricke (or Atkin-Lehner) involution $w_{p^r}$, whose modular interpretation goes as follows. If $N' := N/p^r$ then $w_{p^r}$ maps $(E, C_N) = (E, C_{N'} \times C_{p^r})$ to $(E/C_{p^r}, (C_{N'} \mod C_{p^r}) \times E[p^r]/C_{p^r})$. When $N = p^r$ is a power of the prime $p$, one usually writes $X_0^+(p^r)$ for the quotient curve $X_0(p^r)/w_{p^r}$. In that case, the homographic action of $w_{p^r}$ on $\mathcal{H}$ is given by the matrix $\left(\begin{smallmatrix} 0 & -1 \\ p^r & 0 \end{smallmatrix}\right)$. We also define the degeneracy morphism induced by $z \mapsto pz$ on $\mathcal{H}$, with the ugly modular description:

$$\begin{array}{rcl} \pi_{p^{r+2},p^r} : X_0(p^{r+2}) & \longrightarrow & X_0(p^r) \\ (E, C_{p^{r+2}}) & \longmapsto & (E/p^{r+1}C_{p^{r+2}}, pC_{p^{r+2}} \bmod p^{r+1}C_{p^{r+2}}). \end{array}$$

One has $\pi_{p^{r+2},p^r} \circ w_{p^{r+2}} = w_{p^r} \circ \pi_{p^{r+2},p^r}$. This is for instance readily checked on the quotients of $\bar{\mathcal{H}}$, so it is true over $\mathbb{Z}$, therefore over any base. It follows

that $\pi_{p^{r+2},p^r}$ induces a degeneracy morphism

$$\pi^+_{p^{r+2},p^r}\colon X_0^+(p^{r+2}) \to X_0^+(p^r) \tag{2.1}$$

already alluded to in our introduction.

In the present text our main object of study will be the case when $N = p$ is a prime number and $G$ is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ (resp. the normalizer of a split Cartan), that is a group conjugate to the diagonal subgroup (resp. the subgroup of diagonal and anti-diagonal elements). The corresponding modular curve will be denoted by $X_{\mathrm{sp.C}}(p)$ (resp. $X_{\mathrm{split}}(p)$). It parameterizes geometric isomorphism classes of elliptic curves endowed with an ordered pair (resp. an unordered pair) of independent $p$-isogenies. Factorizing by the natural involution $w$ that switches the isogenies (which is induced by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ acting on the Poincaré half-plane $\mathcal{H}$) defines a degree 2 covering $X_{\mathrm{sp.C}}(p) \to X_{\mathrm{split}}(p)$.

Although the curves $X_0(N)$ and $X_{\mathrm{sp.C}}(p)$ look quite different they are known to be linked, in the following somewhat unintuitive way. One checks that for any $s \geqslant 0$ the map $z \mapsto p^s z$ on Poincaré upper half-plane defines an analytic isomorphism $\varphi_s\colon X_0(p^{2s}) \to X_{\mathrm{sp.C}}(p^s)$, with the obvious generalization of definitions. The modular interpretation of $\varphi_s$ is quite twisted, but it is an elementary exercise on the interpretation of lattices in $\mathbb{C}$ to check that

$$\varphi_s\colon \big(E_1, f\colon E_1 \longrightarrow E_2\big) \mapsto \big(E, \big(\phi^*\colon E \longrightarrow E_1, \psi\colon E \longrightarrow E_2\big)\big), \tag{2.2}$$

where $\psi \circ \phi\colon E_1 \longrightarrow E \longrightarrow E_2$ is the obvious decomposition of the cyclic $p^{2s}$-isogeny $f\colon E_1 \longrightarrow E_2$ into the product of two $p^s$-isogenies and $\phi^*$ is the dual isogeny. This again shows that $\varphi_s$ comes from a scheme morphism over $\mathbb{Q}$ (or $\mathbb{Z}$). It is moreover straightforward to check that $\varphi_s \circ w_{p^{2s}} = w \circ \varphi_s$ so $\varphi_s$ induces a $\mathbb{Q}$-(or $\mathbb{Z}$-)isomorphism:

$$\varphi_s^+\colon X_0^+(p^{2s}) \to X_{\mathrm{split}}(p^s). \tag{2.3}$$

Of course the natural degeneracy maps $X_{\mathrm{split}}(p^{s+1}) \to X_{\mathrm{split}}(p^s)$ obtained by reducing mod $p^s$ the $p^{s+1}$-level structure translates into the degeneracy morphisms $X_0^+(p^{2s+2}) \to X_0^+(p^{2s})$ introduced in (2.1), in the case of even powers of $p$.

We define the naive Weil height $\mathrm{h}(P)$ of any point $P$ in $X_G(\bar{\mathbb{Q}})$ as the height of the algebraic number $j(P)$, that is, the height of the $j$-invariant of any elliptic curve in the isomorphism class defined by $P$:

$$\mathrm{h}(P) = \mathrm{h}(j) = [K\colon \mathbb{Q}]^{-1} \sum_v [K_v\colon \mathbb{Q}_v] \log \max\{|j|_v, 1\}$$

where $K$ is any number field containing $j$, the sum runs through all places $v$ of $K$ (normalized to extend the usual valuations of $\mathbb{Q}$) and $K_v$, $\mathbb{Q}_v$ denote the obvious completions. The value of $\mathrm{h}(j)$ is known to be independent on the particular choice of $K$. If $j$ is a rational integer or an imaginary quadratic integer then $\mathrm{h}(j) = \log|j|$. We also use Faltings heights at some point, but we recall their properties relevant to us when needed.

## 3. Explicit bounds for integral points

In this section we prove the following explicit version of Theorem 1.1 from [6] (see Subsection 3.3).

THEOREM 3.1. — *For any prime number $p \geqslant 3$ and any $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$ we have*

$$\mathrm{h}(P) = \mathrm{h}(j_P) \leqslant 2\pi p^{1/2} + 6\log p + 21(\log p)^2 p^{-1/2}. \tag{3.1}$$

Here constants $2\pi$ and 6 are best possible for the method, but 21 can be refined, and can be replaced by 3 for sufficiently large $p$.

The $\mathbb{Q}$-isomorphism $X_{\mathrm{split}}(p) \simeq X_0^+(p^2)$ given by (2.3) when $s = 1$ shows that Theorem 3.1 allows one to tackle the case $r = 2$ in Theorem 1.1. To deal with the case $r = 3$, we will further need the following result, which is Theorem 6.1 from [5].

THEOREM 3.2. — *Let $p \geqslant 3$ be a prime number and $K$ a number field of degree at most 2 with ring of integers $\mathcal{O}_K$. Then for a point $P \in Y_{\mathrm{sp.C}}(p)(\mathcal{O}_K)$ we have $\mathrm{h}(P) \leqslant 24p\log(3p)$.*

To prove Theorem 3.1, we follow the arguments of [6] and [5], making explicit all the constants occurring therein. We shall routinely use the inequality[(1)]

$$\bigl|\log(1+z)\bigr| \leqslant -\frac{\log(1-r)}{r}|z| \qquad \text{for } |z| \leqslant r < 1. \tag{3.2}$$

### 3.1. Siegel Functions

For $\tau \in \mathcal{H}$ we, as usual, put $q = q(\tau) = e^{2\pi i\tau}$. For a rational number $a$ we define $q^a = e^{2\pi i a\tau}$. Let $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ be such that $\mathbf{a} \notin \mathbb{Z}^2$, and let

(1) We choose the principal determination of the logarithm, that is, for $z \in \mathbb{C}$ satisfying $|z| < 1$, we set $\log(1+z) := -\sum_{k=1}^{\infty}(-z)^k/k$.

$g_{\mathbf{a}}\colon \mathcal{H} \to \mathbb{C}$ be the corresponding *Siegel function* [20, Section 2.1]. Then we have the following infinite product presentation for $g_{\mathbf{a}}$ [20, page 29]:

(3.3)
$$g_{\mathbf{a}}(\tau) = -q^{B_2(a_1)/2} e^{\pi i a_2 (a_1 - 1)} \prod_{n=0}^{\infty} \left(1 - q^{n+a_1} e^{2\pi i a_2}\right) \left(1 - q^{n+1-a_1} e^{-2\pi i a_2}\right),$$

where $B_2(T) = T^2 - T + 1/6$ is the second Bernoulli polynomial.

The following is a quantitative version of (slightly modified) Proposition 2.1 from [6]. Let $D$ be the familiar fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$ (that is, the hyperbolic triangle with vertices $e^{\pi i/3}$, $e^{2\pi i/3}$ and $i\infty$, together with the geodesic segments $[i, e^{2\pi i/3}]$ and $[e^{2\pi i/3}, i\infty]$) and $D + \mathbb{Z}$ the union of all translates of $D$ by the rational integers.

PROPOSITION 3.3. — *Assume that $0 \leqslant a_1 < 1$. Then for $\tau \in D + \mathbb{Z}$ we have*

$$\log |g_{\mathbf{a}}(\tau)| = \frac{1}{2} B_2(a_1) \log |q| + \log \left|1 - q^{a_1} e^{2\pi i a_2}\right| + \log \left|1 - q^{1-a_1} e^{-2\pi i a_2}\right| + O_1(3|q|).$$

*Proof.* — We only have to show that

$$\left| \sum_{n=1}^{\infty} \left( \log \left|1 - q^{n+a_1} e^{2i\pi a_2}\right| + \log \left|1 - q^{n+1-a_1} e^{-2i\pi a_2}\right| \right) \right| \leqslant 3|q|.$$

But this is inequality (11) from [5]. We may notice that in [5] it is assumed that $\tau \in D$, but what is actually used is the inequality $|q(\tau)| \leqslant e^{-\pi\sqrt{3}}$, which holds for every $\tau \in D + \mathbb{Z}$. □

### 3.2. A Modular Unit

In this subsection we briefly recall the "modular unit" construction. See [6, Section 3] for more details.

Let $N$ be a positive integer. Then for $\mathbf{a}, \mathbf{a}' \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$ such that $\mathbf{a} \equiv \mathbf{a}' \bmod \mathbb{Z}^2$, we have $g_{\mathbf{a}}^{12N} = g_{\mathbf{a}'}^{12N}$. Hence the function $g_{\mathbf{a}}^{12N}$ is well-defined for $\mathbf{a} \in \left(N^{-1}\mathbb{Z}/\mathbb{Z}\right)^2 \smallsetminus \{0\}$. The function $u_{\mathbf{a}} = g_{\mathbf{a}}^{12N}$ is $\Gamma(N)$-automorphic and hence defines a rational function on the modular curve $X(N)$; in fact, it belongs to the field $\mathbb{Q}(\zeta_N)\big(X(N)\big)$.

Now assume that $N = p \geqslant 3$ is an odd prime number, and denote by $p^{-1}\mathbb{F}_p^{\times}$ the set of non-zero elements of $p^{-1}\mathbb{Z}/\mathbb{Z}$. Put

$$A = \left\{(a, 0)\colon a \in p^{-1}\mathbb{F}_p^{\times}\right\} \cup \left\{(0, a)\colon a \in p^{-1}\mathbb{F}_p^{\times}\right\}, \quad U = \prod_{\mathbf{a} \in A} u_{\mathbf{a}}.$$

Then $U$ is $\Gamma_{\mathrm{split}}(p)$-automorphic; in particular, it defines a rational function on $X_{\mathrm{split}}(p)$, also denoted by $U$; in fact, $U \in \mathbb{Q}(X_{\mathrm{split}}(p))$.

More generally, for $c \in \mathbb{Z}$ put

$$\beta_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \qquad U_c = U \circ \beta_c = \prod_{\mathbf{a} \in A\beta_c} u_{\mathbf{a}}$$

(recall that $u_{\mathbf{a}} \circ \gamma = u_{\mathbf{a}\gamma}$), so that $U = U_0$. (Warning: for $c$ non-divisible by $p$ the function $U_c$ is not $\Gamma_{\mathrm{split}}(p)$-automorphic!) The following is a quantitative version of Proposition 3.3 from [6].

PROPOSITION 3.4. — *For $\tau \in D + \mathbb{Z}$ we have*

$$\log|U_c(\tau)| = \begin{cases} (p-1)^2 \log|q| + O_1\left(4\pi^2 \dfrac{p^2}{\log|q^{-1}|} + 12p\log p + 77p^2|q|\right) & \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } p \mid c, & \\ -2(p-1)\log|q| + O_1\left(8\pi^2 \dfrac{p^2}{\log|q^{-1}|} + 72p^2|q|\right) \quad \text{if } p \nmid c, & \end{cases}$$

*where we write $q = q(\tau)$.*

For the proof of Proposition 3.4 we need a slight sharpening of Lemma 3.5 from [6].

LEMMA 3.5. — *Let $z$ be a complex number, $0 < |z| < 1$, and $N$ a positive integer. Then*

$$\left|\sum_{k=1}^{N} \log\bigl|1 - z^k\bigr|\right| \leqslant \frac{\pi^2}{6} \frac{1}{\log|z^{-1}|}. \tag{3.4}$$

*Proof.* — We have $\bigl|\log|1+z|\bigr| \leqslant -\log(1-|z|)$ for $|z| < 1$. Hence it suffices to prove the inequality

$$-\sum_{k=1}^{\infty} \log(1-q^k) \leqslant \frac{\pi^2}{6} \frac{1}{\log(q^{-1})} \qquad (0 < q < 1). \tag{3.5}$$

Using (3.2) with $-q^k$ instead of $z$ and with $r = 1/2$, we find that for $0 < q \leqslant 1/2$

$$-\sum_{k=1}^{\infty} \log(1-q^k) \leqslant (4\log 2)q \leqslant \frac{4\log 2}{e} \frac{1}{\log(q^{-1})} < \frac{\pi^2}{6} \frac{1}{\log(q^{-1})},$$

which proves (3.5) for $0 < q \leqslant 1/2$. We are left with $1/2 \leqslant q < 1$.

Put $\tau = \log q/(2\pi i)$. Then

$$-\sum_{k=1}^{\infty} \log(1-q^k) = \frac{1}{24}\log q - \log|\eta(\tau)|,$$

where $\eta(\tau)$ is the Dedekind $\eta$-function. Since $|\eta(\tau)| = |\tau|^{-1/2}|\eta(-\tau^{-1})|$, we have

$$-\sum_{k=1}^{\infty}\log(1-q^k) = -\frac{1}{24}\log Q + \frac{1}{24}\log q + \frac{1}{2}\log|\tau| - \sum_{k=1}^{\infty}\log(1-Q^k) \tag{3.6}$$

with $Q = e^{-2\pi i\tau^{-1}} = e^{4\pi^2/\log q}$. The first term on the right of (3.6) is exactly $(\pi^2/6)/\log(q^{-1})$, and the second term is negative for $0 < q < 1$. To complete the proof, we must show that, when $1/2 \leqslant q < 1$, the sum of the remaining two terms is negative.

Indeed, when $1/2 \leqslant q < 1$, we have

$$\frac{1}{2}\log|\tau| \leqslant -\frac{1}{2}\log\frac{2\pi}{\log 2} \leqslant -1, \qquad Q \leqslant e^{-4\pi^2/\log 2} \leqslant 10^{-24}.$$

Applying (3.2) with $-Q^k$ instead of $z$ and with $r = 10^{-24}$, we bound the fourth term in (3.6) by $10^{-23}$. Hence the sum of the third and the fourth terms is negative, as wanted. □

*Proof of Proposition 3.4.* — For $a \in \mathbb{Q}/\mathbb{Z}$ we denote by $\tilde{a}$ the lifting of $a$ to the interval $[0,1)$. Then for $\tau \in D + \mathbb{Z}$ we deduce from Proposition 3.3 that

$$\log|U_c(\tau)| = 6p\Sigma_1\log|q| + 12p\Sigma_2 + O_1(72p^2|q|), \tag{3.7}$$

where

$$\Sigma_1 = \sum_{\mathbf{a}\in A\beta_c} B_2(\tilde{a}_1),$$

$$\Sigma_2 = \sum_{\mathbf{a}\in A\beta_c} \Big(\log\big|1 - q^{\tilde{a}_1}e^{2\pi i a_2}\big| + \log\big|1 - q^{1-\tilde{a}_1}e^{-2\pi i a_2}\big|\Big).$$

Now we are going to calculate $\Sigma_1$, using the identity

$$\sum_{k=1}^{N-1} B_2\left(\frac{k}{N}\right) = -\frac{(N-1)}{6N},$$

and to estimate $\Sigma_2$ using Lemma 3.5.

If $p \mid c$ then $A\beta_c = A$ and

$$\Sigma_1 = \sum_{k=1}^{p-1} B_2\left(\frac{k}{p}\right) + (p-1)B_2(0) = \frac{(p-1)^2}{6p}, \tag{3.8}$$

$$\Sigma_2 = 2\sum_{k=1}^{p-1}\log\big|1 - q^{k/p}\big| + \log\left|\frac{1-q^p}{1-q}\right| + \log p. \tag{3.9}$$

Lemma 3.5 with $z = q^{1/p}$ implies that

$$\Big|\sum_{k=1}^{p-1} \log|1 - q^{k/p}|\Big| \leqslant \frac{\pi^2}{6}\frac{p}{\log|q^{-1}|}.$$

Also, since $|q| \leqslant e^{-\pi\sqrt{3}}$, we have $\Big|\log|1-q|\Big| \leqslant 1.01|q|$ and

$$\Big|\log|1-q^p|\Big| \leqslant 1.01|q|^p \leqslant 0.01|q|.$$

Combining all this with (3.7), (3.8) and (3.9), we prove the proposition in the case $p \mid c$.

If $p \nmid c$ then $A\beta_c = \{(a,0)\colon a \in p^{-1}\mathbb{F}_p^\times\} \cup \{(a,ab)\colon a \in p^{-1}\mathbb{F}_p^\times\}$, where $bc \equiv 1 \bmod p$. Hence

$$\Sigma_1 = 2\sum_{k=1}^{p-1} B_2\left(\frac{k}{p}\right) = -\frac{p-1}{3p},$$

$$\Sigma_2 = 2\sum_{k=1}^{p-1} \log\big|1 - q^{k/p}\big| + 2\sum_{k=1}^{p-1} \log\big|1 - (q^{1/p}e^{2\pi ib/p})^k\big|.$$

Using Lemma 3.5 with $z = q^{1/p}$ and with $z = q^{1/p}e^{2\pi ib/p}$, we complete the proof. □

### 3.3. Proof of Theorem 3.1

We set $G$ as the subgroup of diagonal and anti-diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ and choose the corresponding modular curve as a model for $X_{\mathrm{split}}(p)$. Define the "modular units" $U_c$ as in Subsection 3.2. Recall that $U = U_0$ belongs to the field $\mathbb{Q}(X_{\mathrm{split}}(p))$. Theorem 3.1 will be a consequence of Proposition 3.4 and the following statement, which is Proposition 4.2 from [6].

PROPOSITION 3.6. — *For $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$ we have*

$$0 \leqslant \log|U(P)| \leqslant 24p\log p.$$

We are ready now to prove Theorem 3.1. Let $p \geqslant 3$ and $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$. According to Lemma 3.2 from [6], there exists $\tau \in D + \mathbb{Z}$ and $c \in \mathbb{Z}$ with $U_c(\tau) = U(P)$ and $j(\tau) = j(P)$. We write $q = q(\tau)$. Recall that $j(\tau)$ and $q(\tau)$ are real numbers, and that $\mathrm{h}(j(\tau)) = \log|j(\tau)|$ if $j(\tau) \in \mathbb{Z}$. It suffices to show that

$$\log|q^{-1}| \leqslant 2\pi p^{1/2} + 6\log p + 20(\log p)^2 p^{-1/2}. \tag{3.10}$$

Indeed, we may assume that $|j(\tau)| \geqslant 3500$ (otherwise (3.1) holds trivially), in which case Corollary 2.2 of [5] gives $\left|j(\tau) - q^{-1}\right| \leqslant 1100$. Hence, using the inequality

$$\log|a| \leqslant \log|b| + \frac{|a-b|}{|a| - |a-b|},$$

which holds for real numbers $a$ and $b$ with same sign (and $0 < |b| < |a|$ or $0 < |a| < |b| < |2a|$), we obtain

$$\log|j(\tau)| \leqslant \log|q^{-1}| + \frac{1100}{|j(\tau)| - 1100}.$$

Now using (3.10) and assuming that $\log|j(\tau)| \geqslant 2\pi p^{1/2} + 6\log p$, we obtain

$$\begin{aligned}\log|j(\tau)| &\leqslant 2\pi p^{1/2} + 6\log p + 20\frac{(\log p)^2}{p^{1/2}} + \frac{1100}{p^6 e^{2\pi p^{1/2}} - 1100}\\ &\leqslant 2\pi p^{1/2} + 6\log p + 21\frac{(\log p)^2}{p^{1/2}},\end{aligned}$$

as wanted.

Let us prove (3.10). Assume first that $p \nmid c$. Using Propositions 3.4 and 3.6 and assuming that $\log|q^{-1}| \geqslant 2\pi p^{1/2} + 6\log p$, we obtain

$$\begin{aligned}\log|q^{-1}| &\leqslant \frac{\log|U_c(\tau)|}{2(p-1)} + \frac{4\pi^2 p^2}{p-1}\frac{1}{\log|q^{-1}|} + 36\frac{p^2}{p-1}|q|\\ &\leqslant \frac{12p\log p}{p-1} + \frac{4\pi^2 p}{\log|q^{-1}|} + \frac{4\pi^2 p}{p-1}\frac{1}{\log|q^{-1}|} + 54p|q|\\ &\leqslant 12\log p + \frac{12\log p}{p-1} + \frac{4\pi^2 p}{\log|q^{-1}|} + \frac{2\pi p^{1/2}}{p-1} + 54p^{-5}e^{-2\pi p^{1/2}}\\ &\leqslant 12\log p + \frac{4\pi^2 p}{\log|q^{-1}|} + \frac{21}{p^{1/2}}.\end{aligned}$$

It follows that $\log|q^{-1}|$ does not exceed the largest root of the quadratic polynomial

$$f(T) = T^2 - \left(12\log p + 21p^{-1/2}\right)T - 4\pi^2 p,$$

that is,

$$\begin{aligned}\log|q^{-1}| &\leqslant \left(4\pi^2 p + \left(6\log p + 10.5p^{-1/2}\right)^2\right)^{1/2} + 6\log p + 10.5p^{-1/2}\\ &\leqslant 2\pi p^{1/2} + \frac{\left(6\log p + 10.5p^{-1/2}\right)^2}{4\pi p^{1/2}} + 6\log p + 10.5p^{-1/2} \qquad (3.11)\\ &\leqslant 2\pi p^{1/2} + 6\log p + 20(\log p)^2 p^{-1/2},\end{aligned}$$

where we use the inequality $(a+b)^{1/2} \leqslant a^{1/2} + (1/2)ba^{-1/2}$ in (3.11). This completes the proof of (3.10) in the case $p \nmid c$.

In the case $p \mid c$ Proposition 3.4 gives

$$\log|q^{-1}| \leqslant -\frac{\log|U_c(\tau)|}{(p-1)^2} + \frac{4\pi^2 p^2}{(p-1)^2}\frac{1}{\log|q^{-1}|} + \frac{12p\log p}{(p-1)^2} + \frac{77p^2}{(p-1)^2}|q|.$$

Proposition 3.6 implies that $-\log|U_c(\tau)| \leqslant 0$. Assuming that

$$\log|q^{-1}| \geqslant 2\pi p^{1/2} + 6\log p,$$

we obtain

$$\log|q^{-1}| \leqslant \frac{2\pi p^{3/2}}{(p-1)^2} + \frac{12p\log p}{(p-1)^2} + \frac{77}{(p-1)^2 p^4} e^{-2\pi p^{1/2}} \leqslant 19,$$

which is sharper than (3.10). The theorem is proved. □

## 4. An Upper Bound for $p$

The main result of this section is the following

Theorem 4.1.

(i) *For $p > 1.4 \cdot 10^7$, every point in $X_0^+(p^2)(\mathbb{Q})$ is either a CM point or a cusp.*

(ii) *For $p > 1.7 \cdot 10^{11}$, every point in $X_0^+(p^3)(\mathbb{Q})$ is either a CM point or a cusp.*

It is an explicit version of Theorem 1.3 from [5], which covers Theorem 1.2 from [6]. Our previous work relied on Pellarin's refinement [30] of Masser-Wüstholz famous upper bound [21] for the smallest degree of an isogeny between two elliptic curves. Here we invoke the following very recent improvement on Pellarin's bound, due to Gaudron and Rémond [15, Theorem 1.4]. We denote by $\mathrm{h}_{\mathcal{F}}(E)$ the semi-stable Faltings height of an elliptic curve $E$ (see [15, Section 2.3], for a discussion on different normalization choices; our $\mathrm{h}_{\mathcal{F}}$ is the $\mathrm{h}_F$ of loc. cit. or the original height of [12]).

Theorem 4.2 (Gaudron and Rémond). — *Let $E$ be an elliptic curve defined over a number field $K$ of degree $d$. Let $E'$ be another elliptic curve, defined over $K$ and isogenous to $E$ over $\bar{K}$. Then there exists an isogeny $\psi\colon E \to E'$ of degree at most $10^7 d^2\big(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\log d\big)^2$.*

Using our Theorem 3.1, Gaudron and Rémond also obtain in [15] a version of item (i) of Theorem 4.1, which is even numerically sharper than ours. However, our version is completely sufficient for our purposes.

We shall use Theorem 4.2 through its following immediate consequence.

PROPOSITION 4.3. — *Let $E$ be a non-CM elliptic curve defined over a number field $K$ of degree $d$, and admitting a cyclic isogeny over $K$ of degree $\delta$. Then $\delta \leqslant 10^7 d^2 \big(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\log d\big)^2$.*

*Proof.* — See for instance [6], Corollary 5.4. □

To prove Theorem 4.1, we shall also need some basic estimates concerning the Faltings height.

PROPOSITION 4.4.

(i) *Let $E$ and $E'$ be isogenous elliptic curves over some number field, connected by an isogeny of degree $\delta$. Then*

$$|\mathrm{h}_{\mathcal{F}}(E) - \mathrm{h}_{\mathcal{F}}(E')| \leqslant (1/2)\log\delta.$$

(ii) *For an elliptic curve $E$ we have $\mathrm{h}_{\mathcal{F}}(E) \leqslant (1/12)\mathrm{h}(j_E) + 3$.*

Item (i) is a well-known result of Faltings [12, Lemma 5]. Item (ii) is, basically, due to Silverman [34, Proposition 2.1], who proved the inequality $\mathrm{h}_{\mathcal{F}}(E) \leqslant (1/12)\mathrm{h}(j_E) + C$ with an unspecified absolute constant $C$. The calculations of Pellarin on pages 240–241 of [30] imply that $C = 4$ would do, though he does not state this explicitly. It finally follows from Gaudron and Rémond [15, Lemma 7.9] that one can take $C = 3$.

We will now combine Theorems 3.1, 3.2 and 4.2 and Proposition 4.4 to prove Theorem 4.1.

*Proof of Theorem 4.1.* — Recall that we have defined in Section 2 an exotic $\mathbb{Q}$-isomorphism $X_0(p^2) \to X_{\mathrm{sp.C}}(p)$, which descends to the isomorphism $X_0^+(p^2) \to X_{\mathrm{split}}(p)$ (equation (2.3)). This interplay between isomorphic curves might look a bit confusing at first sight, but each point of view has its own advantages. In particular, replacing $X_0(p^2)$ by $X_{\mathrm{sp.C}}(p)$ (that is, a level $p^2$-structure by a $p$-structure) is significantly more advantageous for Runge's method.

*Proof of item (i).* Let $Q$ be a non-cuspidal and non-CM point in $X_0^+(p^2)(\mathbb{Q})$, and let $P$ be the corresponding point in $X_{\mathrm{split}}(p)(\mathbb{Q})$ defined by (2.3). Let $E_1$ and $E_2$ be the elliptic curves corresponding to $Q$ (defined over a quadratic extension of $\mathbb{Q}$) and let $E$ be the elliptic curve associated with $P$.

Since $E$ and $E_1$ are $p$-isogenous, Proposition 4.4 implies that

$$\mathrm{h}_{\mathcal{F}}(E_1) \leqslant \mathrm{h}_{\mathcal{F}}(E) + \frac{1}{2}\log p \leqslant \frac{1}{12}\mathrm{h}(j_E) + \frac{1}{2}\log p + 3. \tag{4.1}$$

A result of Mazur, Momose and Merel (see Theorem 6.1 in [6]) implies that $j(P) = j_E \in \mathbb{Z}$; in particular, $\mathrm{h}(j_E) = \log|j_E|$. Hence we may use Theorem 3.1, which yields

$$\frac{1}{12}\mathrm{h}(j_E) \leqslant \frac{2\pi}{12}p^{1/2} + \frac{1}{2}\log p + \frac{21}{12}\frac{(\log p)^2}{p^{1/2}}. \tag{4.2}$$

On the other hand, since $E_1$ admits a cyclic $p^2$-isogeny over a quadratic field, Proposition 4.3 implies that

$$p^2 \leqslant 4\cdot 10^7\bigl(\max\{\mathrm{h}_{\mathcal{F}}(E_1), 985\} + 4\log 2\bigr)^2.$$

Hence $p \leqslant 7\cdot 10^3 \max\{\mathrm{h}_{\mathcal{F}}(E_1), 985\}$, that is, either $p \leqslant 7\cdot 10^6$ and we are done, or $p \leqslant 7\cdot 10^3 \mathrm{h}_{\mathcal{F}}(E_1)$. In this latter case, using (4.1) and (4.2), we obtain

$$p \leqslant 7\cdot 10^3\left(\frac{2\pi}{12}p^{1/2} + \log p + 3 + \frac{21}{12}\frac{(\log p)^2}{p^{1/2}}\right). \tag{4.3}$$

One readily checks that for $p \geqslant 10^7$ the right-hand side of (4.3) does not exceed $3.71\cdot 10^3 p^{1/2}$, which implies that $p \leqslant 1.4\cdot 10^7$. This proves item (i).

*Proof of item (ii).* Let $Q$ be a non-CM non-cuspidal point on $X_0^+(p^3)(\mathbb{Q})$. Let $Q_1$ be one of its lifts in $Y_0(p^3)(K)$, where $K$ is a quadratic field and $Q_2 \in Y_0(p^2)(K)$ its image by the natural morphism $X_0(p^3) \to X_0(p^2)$ which preserves the $j$-invariant. Denote by $P$ the point in $X_{\mathrm{sp.C}}(p)(K)$ corresponding to $Q_2$ via (2.2). Let $E_1$ (resp. $E$) the underlying elliptic curve corresponding to $Q_1$ and $Q_2$ (resp. $P$).

By Theorem 8.1 of [5] we still know that $j(P) = j_E$ belongs to $\mathcal{O}_K$. Theorem 3.2 applied to the point $P$ gives

$$\mathrm{h}(P) = \mathrm{h}(j_E) \leqslant 24p\log(3p). \tag{4.4}$$

Since $E_1$ is $p$-isogenous to $E$, we again have (4.1). Combining it with (4.4), we obtain

$$\mathrm{h}_{\mathcal{F}}(E_1) \leqslant 2p\log(3p) + \frac{1}{2}\log p + 3 \leqslant 2p\log p + 4p. \tag{4.5}$$

On the other hand, the curve $E_1$ is also endowed with a cyclic isogeny of degree $p^3$ over $K$. Proposition 4.3 gives

$$p^{3/2} \leqslant 7\cdot 10^3 \max\{\mathrm{h}_{\mathcal{F}}(E_1), 985\}. \tag{4.6}$$

So now either

$$p \leqslant (7\cdot 10^6)^{2/3} < 4\cdot 10^4$$

and we are done, or $p^{3/2} \leqslant 7\cdot 10^3 \mathrm{h}_{\mathcal{F}}(E_1)$. In the latter case, (4.5) implies that $p^{1/2} \leqslant 7\cdot 10^3(2\log p + 4)$, which can be re-written as

$$ep^{1/2} \leqslant 2.8\cdot 10^4 e\log(ep^{1/2})$$

(where $e = 2.718\ldots$). Since $x/\log x \geqslant 2.8 \cdot 10^4 e$ for $x \geqslant 1.1 \cdot 10^6$, we obtain $ep^{1/2} < 1.1 \cdot 10^6$, which implies $p < 1.7 \cdot 10^{11}$, as wanted. □

## 5. The Heegner-Gross sieve

### 5.1. Reminder on Mazur's method and Heegner-Gross vectors

For the convenience of the reader, here we recall the strategy explained in [29], paragraph 6, refined by the use of generalized jacobians as in the work of Merel [25]. Those results are used in our algorithm. We refer to [29, 31, 25] for details. Everywhere in this section we assume $p \geqslant 11$, $p \neq 13$.

Let $r > 1$ be an integer and $P$ a non-cuspidal and non-CM rational point on $X_0^+(p^r)$. The point $P$ gives rise to a point $x \in Y_0(p^r)(K)$ defined over a number field $K$ with $[K\colon \mathbb{Q}] \leqslant 2$. (By Mazur's results [23], the field $K$ is quadratic at least for $p > 37$.) Let us denote by $X_0(p^r) \stackrel{\pi_p}{\to} X_0(p)$ the natural morphism which preserves the $j$-invariant. It is easy to see that, when the points $x_1 = \pi_p \circ w_{p^r}(x)$ and $x_2 = w_p \circ \pi_p(x)$ are equal in $X_0(p)(K)$, then the point $x$ is a CM point, which yields a contradiction. Elaborating on techniques developed by Mazur in [23], we find a criterion under which the equality $x_1 = x_2$ holds for any non-cuspidal rational point $P$.

#### 5.1.1. Formal immersions and the graph method

As in Section 2 we use the same notation $X_0(p)$ for the Deligne-Rapoport model of $X_0(p)$ over $\mathbb{Z}$, that is to say the normalization of $\mathbb{P}^1$ in $X_0(p)$ via $j\colon X_0(p) \longrightarrow X_0(1) \simeq \mathbb{P}^1$ and by $Y_0(p)$ the open affine subscheme obtained by deleting the cusps. Recall that $\mathcal{O}_K$ denotes the ring of integers of $K$ and let $X_0(p)^{\mathrm{sm}}_{\mathcal{O}_K}$ be the smooth part of $X_0(p)_{\mathcal{O}_K} = X_0(p) \times_{\mathbb{Z}} \mathrm{Spec}(\mathcal{O}_K)$ obtained by removing the supersingular points in characteristic $p$. Let $s_1, s_2\colon \mathrm{Spec}(\mathcal{O}_K) \longrightarrow X_0(p)_{\mathcal{O}_K}$ be the sections defined by $x_1, x_2$, respectively. The next Proposition follows from the work of Momose [27] and from [29].

Proposition 5.1.

(i) *In the fibers of characteristic $p$, the sections $s_1$ and $s_2$ are not supersingular points and coincide ;*
(ii) *the field $K$ is a quadratic extension of $\mathbb{Q}$ in which $p$ splits.*

In the sequel, we adopt the notations of [25]: we denote by $J_0(p)^\sharp$ the generalized jacobian of $X_0(p)$ with respect to the set of cusps and by $J_e^\sharp$ the *winding quotient* of $J_0(p)^\sharp$. Let $J_0(p)^\sharp_{\mathcal{O}_K}$ and $J_{e\,\mathcal{O}_K}^\sharp$ be the respective Néron models over $\mathrm{Spec}(\mathcal{O}_K)$. We consider the composition $\phi_P\colon Y_0(p) \to J_e^\sharp$ of the canonical morphism $J_0(p)^\sharp \to J_e^\sharp$ with the Albanese morphism $Y_0(p) \to J_0(p)^\sharp$, associating to a point $Q$ the class of the divisor $[(Q)-(x_1)]$. It follows from integrality results for $P$ (see, for instance, Appendices of [6] and [5]) and from Proposition 5.1 that one can extend $\phi_P$ to a morphism

$$\phi_P\colon Y_0(p)^{\mathrm{sm}}_{\mathcal{O}_K} \longrightarrow J_{e\,\mathcal{O}_K}^\sharp$$

and the images $\phi_P(s_1)$ and $\phi_P(s_2)$ coincide in characteristic $p$. By [25, Proposition 2], any section of the identity component $J_{e\,\mathcal{O}_K}^{\sharp\,0}$ of $J_{e\,\mathcal{O}_K}^\sharp$ is of finite order. Hence, if $\phi_P$ is a formal immersion at $s_1(\mathbb{F}_p)$ then $s_1 = s_2$ so $x_1 = x_2$. See, for instance, [25], Proof of Proposition 6 in Section 4, for a detailed proof of this fact.

Taking into account the properties of the fibers in characteristic $p$ of $X_0(p)_{\mathcal{O}_K}$, one can then give a criterion of formal immersion [29, 25]. Let $\mathcal{S}$ be the finite set of isomorphism classes of supersingular elliptic curves in characteristic $p$. There is an isomorphism between $\mathrm{Cot}_0(J_0(p)^\sharp_{\mathbb{F}_p})$ and $\mathbb{F}_p^{\mathcal{S}}$. Both can be endowed with a structure of Hecke module compatible with this isomorphism. Any $v = \sum_{s\in\mathcal{S}} \lambda_s[s] \in \mathbb{F}_p^{\mathcal{S}}$ corresponds to an element $\omega_v$ of $\mathrm{Cot}_0(J_{e\,\mathbb{F}_p}^\sharp)$ if and only if $I_e^\sharp v = 0$, where we denote by $I_e^\sharp$ the winding ideal of the Hecke algebra (see [25], proof of Proposition 4). Moreover, taking the modular function $j$ as a local parameter for $Y_0(p)_{\mathbb{F}_p}$ in the neighborhood of $s_1(\mathbb{F}_p)$, we have $\mathrm{Cot}(\phi_P)(\omega_v) = \sum_{s\in\mathcal{S}} \frac{\lambda_s}{j(P)-j(s)} dj$. Arguing along these lines, one obtains the following statement [29, 25] (see also [24]).

Proposition 5.2. — *Let $s_1 \in Y_0(p)^{\mathrm{sm}}(\mathbb{Z}_p)$ be a section, $P$ the point obtained by restriction to the generic fiber and $j(P)$ his $j$-invariant. Suppose that there exists $v = \sum_{s\in\mathcal{S}} \lambda_s[s] \in \mathbb{Z}^{\mathcal{S}}$ such that $I_e^\sharp v = 0$ and $\sum_{s\in\mathcal{S}} \frac{\lambda_s}{j(P)-j(s)} \neq 0$ in $\mathbb{F}_{p^2}$. Then $\phi_P$ is a formal immersion at $s_1(\mathbb{F}_p)$.*

With the variant of Mazur's method explained above, this gives the following consequence (see [25, Proposition 6]):

Corollary 5.3 ([29, 25]). — *If for all ordinary invariants $j_0 \in \mathbb{F}_p$, there exists $v = \sum_{s\in\mathcal{S}} \lambda_s[s] \in \mathbb{Z}^{\mathcal{S}}$ such that $I_e^\sharp v = 0$ and $\sum_{s\in\mathcal{S}} \frac{\lambda_s}{j_0-j(s)} \neq 0$ in $\mathbb{F}_{p^2}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all $r > 1$.*

*Remark 5.4.* — The use of generalized jacobians is not necessary (and was not made in [29] nor in [31]), but it allows one to give a neater formulation to the criterion of Proposition 5.6 below. As an illustration, one can

check that under this new form it readily gives triviality of $X_0^+(37^r)(\mathbb{Q})$, $r \geqslant 2$, for instance, whereas the previous version could not deal with this case and we had to invoke instead peculiar studies of level 37 by Hibino, Murabayashi, Momose and Shimura [19, 28], as discussed in Section 6, page 9 of [29].

### 5.1.2. Heegner-Gross vectors

In [29] the second named author made use of a formula of Gross to exhibit some elements $e_D \in \mathbb{Z}^{\mathcal{S}}$ such that $I_e^\sharp e_D = 0$. Let indeed $-D$ be a quadratic imaginary discriminant and $\mathcal{O}_{-D}$ the order of discriminant $-D$. Let $s \in \mathcal{S}$ be the isomorphism class of a supersingular elliptic curve $E_s$ in characteristic $p$. The ring $R_s = \mathrm{End}_{\mathbb{F}_{p^2}}(E_s)$ is a maximal order of the quaternion algebra $\mathcal{B}$ ramified at $p$ and $\infty$. Moreover, the elements of $\mathcal{S}$ are in one-to-one correspondence with the set of maximal orders of $\mathcal{B}$. The quadratic field $L = \mathbb{Q}(\sqrt{-D}) = \mathcal{O}_{-D} \otimes \mathbb{Q}$ embeds in $\mathcal{B}$ if and only if $p$ is ramified or inert in $L$ and we then denote by $h_s(-D)$ the number of optimal embeddings of $\mathcal{O}_{-D}$ in $R_s$ modulo conjugation by $R_s^\times$ (an embedding is optimal if it does not extend to any larger order). We now define

$$e_D = \frac{1}{|\mathcal{O}_{-D}^\times|} \sum_{s \in \mathcal{S}} h_s(-D)[s] \tag{5.1}$$

which we consider as an element of $\frac{1}{12}\mathbb{Z}^{\mathcal{S}}$.

Proposition 5.5 ([29, 25]). — *We have $I_e^\sharp e_D = 0$.*

This is a slightly modified version of Proposition 4.1 of [29], as explained in [25], Proposition 5 and Corollary of Theorem 6 (see Remark 5.4).

The $h_s(-D)$ optimal embeddings of $\mathcal{O}_{-D}$ in $R_s$ modulo conjugation by $R_s^\times$ are in one-to-one correspondence with the pairs $(E, f)$, where $E$ is an elliptic curve with CM by $\mathcal{O}_{-D}$, which are isomorphic to $E_s$ in characteristic $p$ and $f$ is a given isomorphism $\mathcal{O}_{-D} \cong \mathrm{End}(E)$ (see for instance [18]). So for $p$ inert or ramified in $L$, the vector $e_D$ is the sum of isomorphism classes of elliptic curves which are the reduction in characteristic $p$ of elliptic curves having CM by $\mathcal{O}_{-D}$. The differential associated to $e_D$ is then just equal to the mod $p$ logarithmic derivative:

$$\frac{H'_{-D}(j)}{H_{-D}(j)} dj \tag{5.2}$$

where $H_{-D} = \prod_{E;\mathrm{End}(E)\cong\mathcal{O}_{-D}} (X - j(E))$ is the Hilbert class polynomial associated with $-D$. Applying this to Corollary 5.3 we obtain the following criterion (recall we always assume $p \geqslant 11$, $p \neq 13$).

PROPOSITION 5.6. — *If for all ordinary invariants $j_0 \in \mathbb{F}_p$, there exists a quadratic imaginary discriminant $-D < 0$ such that $p$ is inert or ramified in $\mathbb{Q}(\sqrt{-D})$ and $H'_D(j_0) \neq 0$ in $\mathbb{F}_p$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all integers $r > 1$.*

### 5.2. The sieve

Actually, we use an even more restrictive criterion.

COROLLARY 5.7. — *Let $-D$ be a fundamental quadratic imaginary discriminant and $\chi_D$ the associated quadratic Dirichlet character. For a positive integer $c$, write $R_{c,D} := \mathrm{Res}(H'_{-D}, H'_{-c^2D})$ the integer resultant. Suppose that $p \geqslant 11$, $p \neq 13$ is a prime such that $\chi_D(p) = 0$ or $-1$ and*[2] *$p \nmid r_D := \gcd(R_{c,D}; c \in [\![2,7]\!])$. Then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all integer $r > 1$.*

*Proof.* — Let $p$ be a prime as in the proposition. Then there exists $c \in [\![2,7]\!]$ such that $R_{c,D}$ is not divisible by $p$. (This range of conductors is of course only motivated by our computational needs.) So for all ordinary $j_0 \in \mathbb{F}_p$ either $H'_{-D}(j_0)$ or $H'_{-c^2D}(j_0)$ is non-zero. Moreover, $p$ is inert or ramified in $\mathbb{Q}(\sqrt{-D})$. The result follows from Proposition 5.6. □

We are now ready to state our algorithm. Fix an ordered list $\mathcal{D}$ of fundamental quadratic imaginary discriminants: in the sequel, we eventually choose the discriminants $-D$ of class number $h(-D) \leqslant 4$ to obtain Hilbert class polynomials of small degree $\deg(H_{-D}) = h(-D)$ (see Appendix). By Corollary 5.7, if a prime $p \geqslant 11, p \neq 13$ is *not* in the following set $Pb$ related to $\mathcal{D}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all integer $r > 1$:

$$Pb = \big\{p \text{ prime; for all } -D \in \mathcal{D}, (\chi_D(p) = 1 \text{ or } p \mid r_D)\big\}.$$

This set is the (*a priori* non-disjoint) union of the finite subset $P_1$ of primes $p \in Pb$ which divide some $r_D$ for $-D \in \mathcal{D}$ and the subset

$$P_2 = \big\{p \text{ prime; for all } -D \in \mathcal{D}, \chi_D(p) = 1\big\}.$$

We give an algorithm to compute the set $\mathsf{Bad} = P_1 \cap ([\![11, N-1]\!] \smallsetminus \{13\})$ (Part I) and the set $\mathsf{VeryBad} = P_2 \cap ([\![11, N-1]\!] \smallsetminus \{13\})$ (Part II) for a given integer $N > 13$. We then have

($\star$) *if $11 \leqslant p < N, p \neq 13$ is a prime number such that $p \notin \mathsf{Bad}$ and $p \notin \mathsf{VeryBad}$, then $X_0^+(p^r)(\mathbb{Q})$ is trivial for all $r > 1$.*

[2] We use the "French" notation $[\![a, b]\!]$ for the set of integers $x$ satisfying $a \leqslant x \leqslant b$.

**ALGORITHM, part I.** The set $P_1$ is finite and included in the set $P_1'$ of primes $p$ dividing $r_D$ for some $D \in \mathcal{D}$ such that for all $-d$ before $-D$ in the ordered list $\mathcal{D}$, $p \nmid r_d$ and $\chi_d(p) = 1$. We compute the set $P_1' \cap ([\![11, N-1]\!] \setminus \{13\})$ step-by-step by determining the prime factors of $r_D$, for $-D$ going through the list $\mathcal{D}$. We also construct a list Good of primes which is useful within the procedure (see below). Then if $P_1' \cap ([\![11, N-1]\!] \setminus \{13\})$ is not empty, we compute Bad as explained in step (iii).

**Details:**

(i) If the class number $h(-D)$ is one, then $H_{-D}$ is of degree one and monic so $H'_{-D} = 1$. We initialize a list $\mathcal{L}$ of quadratic imaginary discriminants (which will eventually include all the discriminants from $\mathcal{D}$) to

$$\mathcal{L} = \{-3, -4, -7, -8, -11, -19, -43, -67, -163\} = \{-D, h(-D) = 1\}$$

and we initialize Good and Bad to the empty lists.

(ii) Let $-D$ be the first element of $\mathcal{D}$ which does not belong to $\mathcal{L}$. Let $p$ be a prime factor of $r_D$ which is in $[\![11, N-1]\!] \setminus \{13\}$ and not yet in Good nor in Bad. If for all discriminant $-d \in \mathcal{L}$ (that is, $-d$ "before" $-D$ in $\mathcal{D}$) we have $\chi_d(p) = 1$, then we put $p$ in the list Bad; else we put it in Good. We add $-D$ to $\mathcal{L}$ and start again to (ii) with the next $-D$ (unless $\mathcal{L}$ contains all $\mathcal{D}$).

(iii) When $\mathcal{L}$ contains all the discriminants of $\mathcal{D}$ and if Bad is not empty, we perform the obvious safety check: for each $p \in$ Bad, we test whether at least one of the conditions $p | r_D$ or $\chi_D(p) = 1$ holds true for all $-D \in \mathcal{D}$. If it is not the case, we remove $p$ from Bad.

**Results:** For $\mathcal{D}$ the list of fundamental quadratic imaginary discriminants of class number in $[\![1, 4]\!]$ (see Appendix) and $N = 10^{14}$, we obtain Bad $= \varnothing$ at the end of step (ii). (We therefore did not write in Appendix the Sage code for the unnecessary step (iii) above.)

*Remark 5.8.* — An explanation for the above algorithm converging without step (iii) seems to lie in the fact that the set $\mathcal{P}$ of primes dividing some of the $r_D$ is very small: indeed, keeping track of those primes in the above process, one obtains

$$\mathcal{P} = \big\{2, 3, 5, 7, 11, 13, 17, 19, 149, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 101, 103, 107, 109, 127\big\}.$$

So, although we preferred to state our Algorithm in the above systematic way, in the present numerical setting we could of course have first computed $\mathcal{P}$, then ruled out by hand each of its elements (which finally amounts to repeating something like step (ii)).

**ALGORITHM, part II.** We compute the set $\mathsf{VeryBad}$ of primes $p \in [\![11, N-1]\!] \smallsetminus \{13\}$ for which $\chi_D(p) = 1$ for all $-D \in \mathcal{D}$. For this, we refine the "trial and search" naive idea.

(i) We consider a sublist $\mathcal{D}'$ of $\mathcal{D}$ for which we compute explicitly the values of congruences of primes $p$ for which $\chi_D(p) = 1$ for all $-D \in \mathcal{D}'$. In practice, we take

$$\begin{aligned}\mathcal{D}' = \big\{ &-3, -4, -7, -11, -19, -20, -52, -15, -35, -51, -91,\\ &-115, -187, -23, -68, -84, -132, -39, -55, -228, -340,\\ &-532, -195, -203, -1012, -323, -435, -483, -595, -627,\\ &-667, -715\big\}.\end{aligned} \tag{5.3}$$

Since $-4 \in \mathcal{D}'$ and because of the factorization of the composite discriminants of $\mathcal{D}'$ (see Appendix), $\chi_D(p) = 1$ for all $-D \in \mathcal{D}'$ if and only if $p$ is a non-zero square modulo $q$ for all $q$ in the set

$$\mathcal{L}' = \{3, 4, 5, 7, 11, 13, 17, 19, 23, 29\}.$$

(Note that we precisely chose $\mathcal{D}'$ to be the largest subset of $\mathcal{D}$ such that $\mathcal{L}' \smallsetminus \{4\}$ is the list of the first nine odd prime numbers.) We define the product of the elements in $\mathcal{L}'$:

$$M = 3 \cdot 4 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 = 12\,939\,386\,460.$$

There are 1 995 840 residues modulo $M$ which are non-zero squares modulo $q$ for all $q \in \mathcal{L}'$; they form a subset $\mathcal{S}$ of $[\![0, M-1]\!]$. To determine $\mathcal{S}$ we make a list of all non-zero squares modulo $q$ for each $q \in \mathcal{L}'$ and use the Chinese Remainder Theorem.

(ii) For each value $a \in \mathcal{S}$ and each integer $p \equiv a \pmod{M}$ in the range $[\![11, N]\!]$, if $p$ is a pseudoprime[(3)], we test if $\chi_D(p) = 1$ for all $-D \in \mathcal{D} \smallsetminus \mathcal{D}'$. If it is and if $p$ is indeed prime, we put it in $\mathsf{VeryBad}$.

[(3)] Here we say that $p$ is a pseudoprime if it is a Baillie-Pomerance-Selfridge-Wagstaff pseudo prime (strong Rabin-Miller pseudo prime for base 2, followed by strong Lucas test for the sequence $(P, -1)$, where $P$ is the smallest positive integer such that $P^2 - 4$ is not a square mod $p$). This is what is tested by the PARI "ispseudoprime" function; see [1]. Of course, primes are pseudoprimes!

**Results:** With $\mathcal{D}'$ as before and $N = 10^{14}$, we obtain $\mathsf{VeryBad} = \varnothing$.

The output of all that is the following.

PROPOSITION 5.9. — *If $p$ is a prime number, $11 \leqslant p < 10^{14}$ and $p \neq 13$, then $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$ consist of cusps and CM points.*

*Proof.* — Part I of the algorithm implies that $\mathsf{Bad} = \varnothing$, and by Part II we have $\mathsf{VeryBad} = \varnothing$. We conclude by $(\star)$. □

Together with Theorem 4.1 we obtain Theorem 1.1 of the introduction.

COROLLARY 5.10. — *The same conclusion as for Proposition 5.9 is true for $X_0^+(p^r)(\mathbb{Q})$ with $p \geqslant 11$, $p \neq 13$ (and $r > 1$).*

*Remark 5.11.* — We close this paper by discussing the cursed level 13. As explained in the introduction, the question of the rational points on $X_0^+(169) \cong X_{\mathrm{split}}(13)$ is the only remaining open case among the curves $X_0^+(p^r)$ for $r > 1$. We do not prove anything new here, but try to use this "stubbornly resisting" example (according to Darmon's expression) to illustrate in details some of the tools used all over the paper.

First recall that for all prime $p$, the Jacobian $J_{\mathrm{nonsplit}}(p)$ of the curve $X_{\mathrm{nonsplit}}(p)$ associated to the normalizer of a nonsplit Cartan subgroup mod $p$ is isomorphic to the newpart $J_0^{+,\mathrm{new}}(p^2)$ of the Jacobian $J_0^+(p^2)$ of $X_0^+(p^2)$ (see [9]). On the other hand, one knows that $J_0^+(p^2)$ decomposes up to isogeny as

$$J_0^+(p^2) \sim J_0(p) \times J_0^{+,\mathrm{new}}(p^2) \sim J_0(p) \times J_{\mathrm{nonsplit}}(p)$$

(see, for instance, [27], p. 444). The $J_0(p)$ factor in the above decomposition, and, more precisely, its $J_0^-(p)$, $J_e(p)$ and $\tilde{J}(p)$ successive subquotients, play a crucial role in our techniques, as they allow us to use Mazur's method in order to prove integrality of rational points; as is well-known, the absence of such quotients is one of the main problems with the case of $X_{\mathrm{nonsplit}}(p)$ or $X_0^+(p)$.

Now when $p = 13$ one has $J_0(13) = 0$, so the jacobians of $X_{\mathrm{nonsplit}}(p)$ and $X_{\mathrm{split}}(p)$ are isogenous. (For prime levels, this is the only case where this interesting phenomenon occurs, as everything is 0 for $p = 2, 3, 5, 7$, that is, for the other primes $p$ for which $g(X_0(p)) = 0$). Actually more is true: Burcu Baran [3] proved by computing explicit equations that the curves $X_{\mathrm{split}}(13)$ and $X_{\mathrm{nonsplit}}(13)$ are actually *isomorphic* over $\mathbb{Q}$. One therefore now faces difficulties of "nonsplit type". Our curve is of genus 3, and its jacobian should be of the same rank over $\mathbb{Q}$, so not only Mazur's method, but also Chabauty's method is of no help here. The thirteen quadratic imaginary

orders with class number one give rise to seven points in $X_{\mathrm{nonsplit}}(13)(\mathbb{Q})$ and six points in $X_{\mathrm{split}}(13)(\mathbb{Q})$. The rational cusp of the latter restores the balance with $X_{\mathrm{nonsplit}}(13)$. Galbraith [14] and Baran [3] checked that there are no rational points but the trivial ones in a big box, but to conclude that there are no point at all we would need some effective Mordell, at least for that particular curve. Our Theorem 3.1 can still be used as an approximation (to effective Mordell) for *integral* points (it yields that their Weil height $\mathrm{h}(j)$ is bounded above by 76.4, and this can be lowered by optimizing the estimations in the proof of Theorem 3.1), but again we cannot go further because of the lack of integrality results... Perhaps the techniques of [8] could be of some help here.

## 6. Appendix : tables and codes

- **Fundamental quadratic imaginary discriminants of class number in the range $[\![1,4]\!]$ (see [2] )**

  Class number 1:

  $-\{3,4,7,8,11,19,43,67,163\}$

  Class number 2:

  $-\{20,24,40,52,15,88,35,148,51,232,91,115,123,187,235,267,403,427\}$

  Class number 3:

  $-\{23,31,59,83,107,139,211,283,307,331,379,499,547,643,883,907\}$

  Class number 4:

  $-\{56,68,84,120,132,136,39,168,184,55,228,280,292,312,328,340,372,388,408,520,532,568,155,708,760,772,195,203,219,1012,259,291,323,355,435,483,555,595,627,667,715,723,763,795,955,1003,1027,1227,1243,1387,1411,1435,1507,1555\}$

  The ordered list $\mathcal{D}$ used in section 5.2 is the concatenation of the above lists (discriminants of class number 1, ..., discriminants of class number 4).
- **Factorisation of (the opposite of) the composite discriminants in $\mathcal{D}'$:**

| | | | |
|---|---|---|---|
| $4 = 2^2$, | $20 = 2^2 \cdot 5$, | $52 = 2^2 \cdot 13$, | $15 = 3 \cdot 5$, |
| $35 = 5 \cdot 7$, | $51 = 3 \cdot 17$, | $91 = 7 \cdot 13$, | $115 = 5 \cdot 23$, |
| $187 = 11 \cdot 17$, | $68 = 2^2 \cdot 17$, | $84 = 82^2 \cdot 3 \cdot 7$, | $132 = 2^2 \cdot 3 \cdot 11$, |
| $39 = 3 \cdot 13$, | $55 = 5 \cdot 11$, | $228 = 2^2 \cdot 3 \cdot 19$, | $340 = 2^2 \cdot 5 \cdot 17$, |
| $532 = 2^2 \cdot 7 \cdot 19$, | $195 = 3 \cdot 5 \cdot 13$, | $203 = 7 \cdot 29$, | $1012 = 2^2 \cdot 11 \cdot 23$, |
| $323 = 17 \cdot 19$, | $435 = 3 \cdot 5 \cdot 29$, | $483 = 3 \cdot 7 \cdot 23$, | $595 = 5 \cdot 7 \cdot 17$, |
| $627 = 3 \cdot 11 \cdot 19$, | $667 = 23 \cdot 29$, | $715 = 5 \cdot 11 \cdot 13$. | |

- **Factorisation of (the opposite of) the composite discriminants in $\mathcal{D} \smallsetminus \mathcal{D}'$:**

| | | | |
|---|---|---|---|
| $8 = 2^3$, | $24 = 2^3 \cdot 3$, | $40 = 2^3 \cdot 5$, | $88 = 2^3 \cdot 11$, |
| $148 = 2^2 \cdot 37$, | $232 = 2^3 \cdot 29$, | $123 = 3 \cdot 41$, | $235 = 5 \cdot 47$, |
| $267 = 3 \cdot 89$, | $403 = 13 \cdot 31$, | $427 = 7 \cdot 61$, | $56 = 2^3 \cdot 7$, |
| $120 = 2^3 \cdot 3 \cdot 5$, | $136 = 2^3 \cdot 17$, | $168 = 2^3 \cdot 3 \cdot 7$, | $184 = 2^3 \cdot 23$, |
| $280 = 2^3 \cdot 5 \cdot 7$, | $292 = 2^2 \cdot 73$, | $312 = 2^3 \cdot 3 \cdot 13$, | $328 = 2^3 \cdot 41$, |
| $372 = 2^2 \cdot 3 \cdot 31$, | $388 = 2^2 \cdot 97$, | $408 = 2^3 \cdot 3 \cdot 17$, | $520 = 2^3 \cdot 5 \cdot 13$ |
| $568 = 2^3 \cdot 71$, | $155 = 5 \cdot 31$, | $708 = 2^2 \cdot 3 \cdot 59$, | $760 = 2^3 \cdot 5 \cdot 19$, |
| $772 = 2^2 \cdot 193$, | $219 = 3 \cdot 73$, | $259 = 7 \cdot 37$, | $291 = 3 \cdot 97$, |
| $355 = 5 \cdot 71$, | $555 = 3 \cdot 5 \cdot 37$, | $723 = 3 \cdot 241$, | $763 = 7 \cdot 109$, |
| $795 = 3 \cdot 5 \cdot 53$, | $955 = 5 \cdot 191$, | $1003 = 17 \cdot 59$, | $1027 = 13 \cdot 79$, |
| $1227 = 3 \cdot 409$, | $1243 = 11 \cdot 113$, | $1387 = 19 \cdot 73$, | $1411 = 17 \cdot 83$, |
| $1435 = 5 \cdot 7 \cdot 41$, | $1507 = 11 \cdot 137$, | $1555 = 5 \cdot 311$ | |

- **Algorithms**: We reproduce here the pseudo-codes of the algorithms described in Section 5.2. The original codes have been written with Sage [1]. We used the hilbert_class_polynomial function to compute $H_{-D}$ and the crt function to apply Chinese Remainder Theorem.

**Algorithm, Part I:**
**bad_discrim_and_primes($\mathcal{D}, N$)**

**Require:** A list $\mathcal{D}$ of imaginary quadratic discriminants and an integer $N > 1$ (as in Section 5.2).

set $L \leftarrow [-3, -4, -7, -8, -11, -19, -43, -67, -163]$, Bad $\leftarrow$ [], and Good $\leftarrow$ [].
**for** $-D$ in $\mathcal{D} \smallsetminus \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$ **do**
  set $G \leftarrow H'_{-D}$
  compute the list $\mathcal{P}_D$ of prime factors of $r_D := \gcd\{\mathrm{Res}(G, H'_{-c^2 D}) : c \in [\![2, 7]\!]\}$
  **for** $p$ in $\mathcal{P}_D$ **do**
    **if** $p > 10$ and $p \neq 13$ and $p < N + 1$ and $p$ not in Good and $p$ not in Bad **then**
      **if** $\chi_m(p) = 1$ for all $-m$ in $L$ **then**
        add $p$ to the list Bad
      **else**
        add $p$ to the list Good.
  add $-D$ to the list $L$
**return** $[L, \mathsf{Bad}]$.

**Algorithm, Part II:**

(i) Let $\mathcal{L}'$ be a list of pairwise coprime moduli $d_1, \dots, d_n$ and put $M = \mathrm{lcm}(\mathcal{L}') = d_1 \dots d_n$. The following function returns the non-zero squares modulo all the integers $d_1, \dots, d_n$ as a list of the form $[M, [\text{integers modulo } M]]$.

**squares_congruences($\mathcal{L}'$)**

**Require:** a list $\mathcal{L}'$ of pairwise coprime moduli

1: do a list $[[k^2 \pmod n) \mid k \in \{1, \dots, (n-1)/2\}] : n \in \mathcal{L}']$
2: **return** [lcm($\mathcal{L}'$), Chinese Remainder Theorem applied to the preceeding list].

(ii) Suppose given a list $C = [M, [s_1, \dots, s_r]]$ with $M$ a modulus and $s_1, \dots, s_r$ integers modulo $M$, a list $L$ of quadratic imaginary discriminants, and two integers $n, m$ with $n < m$. The following function gives the prime numbers in range $[n, m[$ which are congruent to some $s_i$ modulo $M$ and which split in all the quadratic fields with discriminant in $L$.

**very_bad_primes($C, L, n, m$)**

**Require:** $C, L, n, m$ as before.

1: $li \leftarrow []$
2: **for** $i \in \{1, \dots, r\}$ **do**
3: $\quad p \leftarrow s_i + \lceil \frac{n - s_i}{M} \rceil M$
4: $\quad$ **while** $p < m$ **do**
5: $\quad\quad$ **if** $p$ is pseudoprime and $\chi_D(p) = 1$ for all $-D \in L$ **then**
6: $\quad\quad\quad$ **if** $p$ is prime **then**
7: $\quad\quad\quad\quad$ add $p$ to the list $li$
8: $\quad\quad p \leftarrow p + M$
9: **return** $li$

**Applying the algorithms:**

1: set $\mathcal{D}$ to be the list of quadratic imaginary discriminants of class number in range $[\![1, 4]\!]$ and set $\mathcal{D}'$ as in (5.3).
2: $[\mathcal{L}, \mathsf{Bad}] \leftarrow$ bad_discrim_and_primes($\mathcal{D}, 10^{14}$)
3: $C \leftarrow$ square_congruences($[3, 4, 5, 7, 11, 13, 17, 19, 23, 29]$)
4: $V \leftarrow$ very_bad_primes($C, \mathcal{D} \setminus \mathcal{D}', 11, 10^{14}$)

Result: for any prime $p \in [11, 10^{14}] \setminus \{13\}$ such that $p \notin \mathsf{Bad} \cup V$, the rational points on $X_0^+(p^r)$ are trivial for all integer $r > 1$.

## BIBLIOGRAPHY


[1] http://www.sagemath.org/.

[2] http://www.numbertheory.org/classnos/.

[3] B. Baran, "An exceptional isomorphism between modular curves of level 13", preprint (available on the author's webpage).

[4] Y. Bilu & M. Illengo, "Effective Siegel's theorem for modular curves", *Bull. Lond. Math. Soc.* **43** (2011), no. 4, p. 673-688, http://arXiv.org/pdf/0905.0418.

[5] Y. Bilu & P. Parent, "Runge's method and modular curves", *Int. Math. Res. Not. IMRN* (2011), no. 9, p. 1997-2027, http://arXiv.org/pdf/0907.3306.

[6] ———, "Serre's uniformity problem in the split Cartan case", *Ann. of Math. (2)* **173** (2011), no. 1, p. 569-584, http://arXiv.org/pdf/0807.4954.

[7] Y. F. Bilu, "Baker's method and modular curves", in *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, Cambridge Univ. Press, Cambridge, 2002, p. 73-88.

[8] N. Bruin & M. Stoll, "The Mordell-Weil sieve: proving non-existence of rational points on curves", *LMS J. Comput. Math.* **13** (2010), p. 272-306.

[9] I. Chen, "Jacobians of modular curves associated to normalizers of Cartan subgroups of level $p^n$", *C. R. Math. Acad. Sci. Paris* **339** (2004), no. 3, p. 187-192.

[10] P. Deligne & M. Rapoport, "Les schémas de modules de courbes elliptiques", in *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Springer, Berlin, 1973, p. 143-316. Lecture Notes in Math., Vol. 349.

[11] N. D. Elkies, "On elliptic $K$-curves", in *Modular curves and abelian varieties*, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, p. 81-91.

[12] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73** (1983), no. 3, p. 349-366.

[13] S. D. Galbraith, "Rational points on $X_0^+(p)$", *Experiment. Math.* **8** (1999), no. 4, p. 311-318.

[14] ———, "Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves", *J. Théor. Nombres Bordeaux* **14** (2002), no. 1, p. 205-219.

[15] E. Gaudron & G. Rémond, "Théorème des périodes et degrés minimaux d'isogénies", submitted http://arXiv.org/pdf/1105.1230, 2011.

[16] J. González, "On the $j$-invariants of the quadratic $\mathbf{Q}$-curves", *J. London Math. Soc. (2)* **63** (2001), no. 1, p. 52-68.

[17] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics, vol. 776, Springer, Berlin, 1980, With an appendix by B. Mazur, iii+95 pages.

[18] ———, "Heights and the special values of $L$-series", in *Number theory (Montreal, Que., 1985)*, CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, p. 115-187.

[19] T. Hibino & N. Murabayashi, "Modular equations of hyperelliptic $X_0(N)$ and an application", *Acta Arith.* **82** (1997), no. 3, p. 279-291.

[20] D. S. Kubert & S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981, xiii+358 pages.

[21] D. W. Masser & G. Wüstholz, "Estimating isogenies on elliptic curves", *Invent. Math.* **100** (1990), no. 1, p. 1-24.

[22] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* (1977), no. 47, p. 33-186 (1978).

[23] ———, "Rational isogenies of prime degree (with an appendix by D. Goldfeld)", *Invent. Math.* **44** (1978), no. 2, p. 129-162.

[24] L. Merel, "Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques", *Duke Math. J.* **110** (2001), no. 1, p. 81-119, With an appendix by E. Kowalski and P. Michel.

[25] ———, "Normalizers of split Cartan subgroups and supersingular elliptic curves", in *Diophantine geometry*, CRM Series, vol. 4, Ed. Norm., Pisa, 2007, p. 237-255.

[26] F. Momose, "Rational points on the modular curves $X_{\mathrm{split}}(p)$", *Compositio Math.* **52** (1984), no. 1, p. 115-137.

[27] ———, "Rational points on the modular curves $X_0^+(p^r)$", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **33** (1986), no. 3, p. 441-466.

[28] F. Momose & M. Shimura, "Lifting of supersingular points on $X_0(p^r)$ and lower bound of ramification index", *Nagoya Math. J.* **165** (2002), p. 159-178.

[29] P. J. R. Parent, "Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$", *Compos. Math.* **141** (2005), no. 3, p. 561-572.

[30] F. Pellarin, "Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques", *Acta Arith.* **100** (2001), no. 3, p. 203-243.

[31] M. Rebolledo, "Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires", *Pacific J. Math.* **234** (2008), no. 1, p. 167-184.

[32] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), no. 4, p. 259-331.

[33] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1, xiv+267 pages.

[34] J. H. Silverman, "Heights and elliptic curves", in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986, p. 253-265.

Manuscrit reçu le 21 juillet 2011,
accepté le 1er décembre 2011.

Yuri BILU & Pierre PARENT
IMB, Université Bordeaux 1
351 cours de la Libération
33405 Talence CEDEX, FRANCE
yuri@math.u-bordeaux1.fr
http://www.math.u-bordeaux1.fr/~yuri/
Pierre.Parent@math.u-bordeaux1.fr

Marusia REBOLLEDO
Université Blaise Pascal Clermont-Ferrand 2
Laboratoire de Mathématiques
Campus universitaire des Cézeaux
63177 Aubière FRANCE
Marusia.Rebolledo@math.univ-bpclermont.fr
http://math.univ-bpclermont.fr/~rebolledo/